Web Apps Dripping With Honey

OWASP Denver and Boulder too!!

April 2020

HARSH TRUTH #1

Bypassing defenses is often very easy

HARSH TRUTH #2

INTLEAK IS REAL

SOC Analyst

Company (redacted)

$30,000 - $45,000 a year

ARCSIGHT, SPLUNK, LOGRHYTHM, QRADAR, ANTIVIRUS, FIREWALLS AND SOURCEFIRE AND SIMILAR TOOLS PREFERRED. Company Company has open positions for…

· Desirable proficiencies:

o Experience migrating from Checkpoint to Palo Alto

o Network Access Control (Forescout preferred)

o RADIUS

o F5

o Secure Routing & Switching

o Cisco AnyConnect & Umbrella

HARSH TRUTH #3

Sales folks want sales

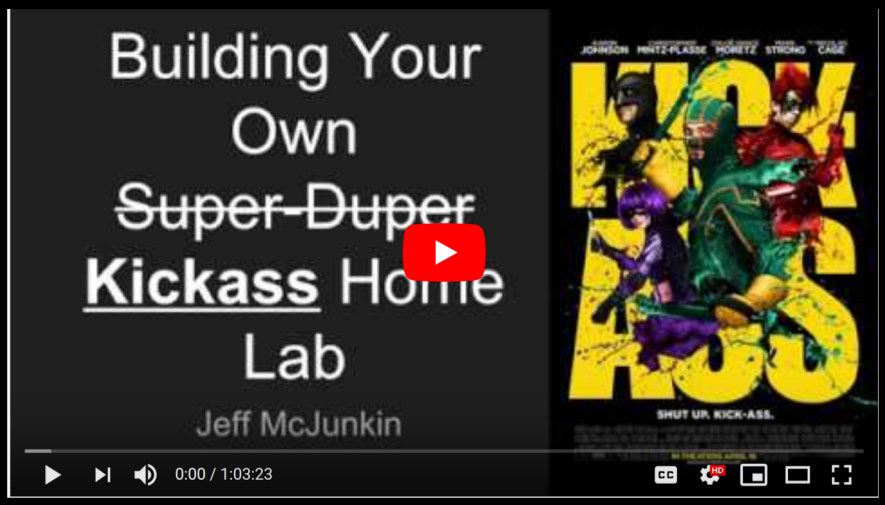
It really is <u>this easy!</u>

A 90-day demo! Heck yeah, we can make that happen!

HARSH TRUTH #4

It’s easier than ever to leverage tech on a PoC

Jeff McJunkin to the rescue



Also, BHIS/AC

HARSH TRUTH #5

PoC will be… *harsh*

SCENE DELETED
(use your imagination)

Recap:

1. **Easy to find your defenses.**
2. **Easy to get your defenses.**
3. **Easy to setup an abuse lab.**

HARSH TRUTH #6

Defenses we all use are *broken*.
But there is another way.

Hi, I'm Mick!

- Managing Partner of InfoSec Innovations
- Teach SANS 504 & 555
- IANS Faculty
- @BetterSafetyNet

What we're going to cover

- Honeypots are dead easy
- Used appropriately, honeypots can be used with existing infrastructure.
- Attackers trip over honeypots
  - They slow attackers down
  - Make for easier detection
  - Make for quicker detection

GOOD TRUTH #1

Attackers expect “normal”

GOOD TRUTH #2

Attackers are predictable

1. Recon
2. Probing
3. Exploitation
4. Post-Exploitation

GOOD TRUTH #3

Honeypots are dead easy…

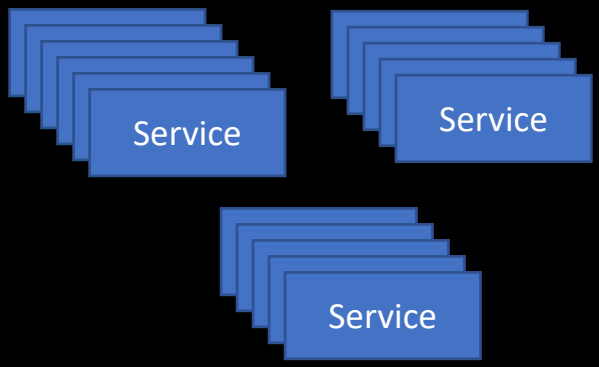
Any interaction is suspect

GOOD TRUTH #4

Web architectures are easy to “honey”

“classic” N-tier architecture

Web services



Honeypots are dead easy…

Honeypots confuse

Confuse recon

PortSpoof

How to run portspoof

Sudo portspoof *** get options here

Honeypots misdirect

Misdirect probes

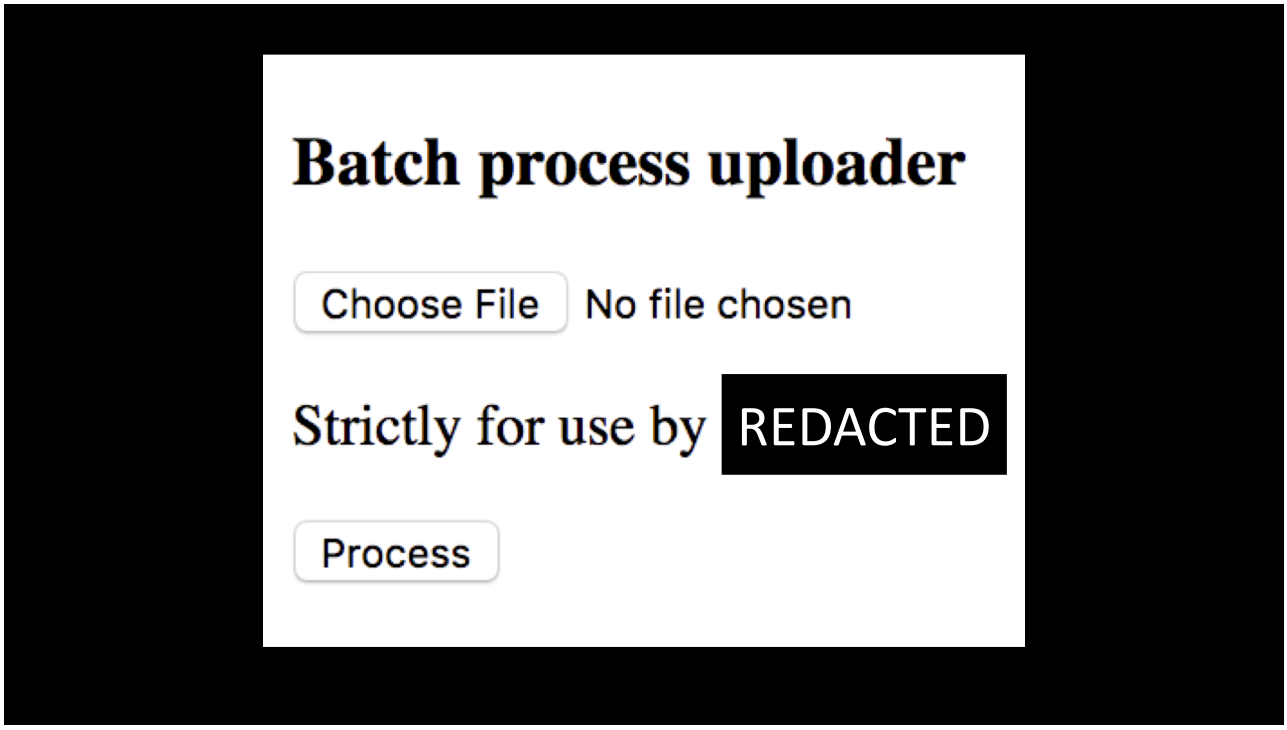
Robots.txt

Honey Robot.txt

```
User-agent: *
Disallow: /api/
Disallow: /bo/
Disallow: /uploader.jsp
Disallow: /admin/
Disallow: /editor.jsp
```

Honey Upload

```
User-agent: *
Disallow: /api/
Disallow: /bo/
Disallow: /uploader.jsp
Disallow: /admin/
Disallow: /editor.jsp
```



Honey User Logon

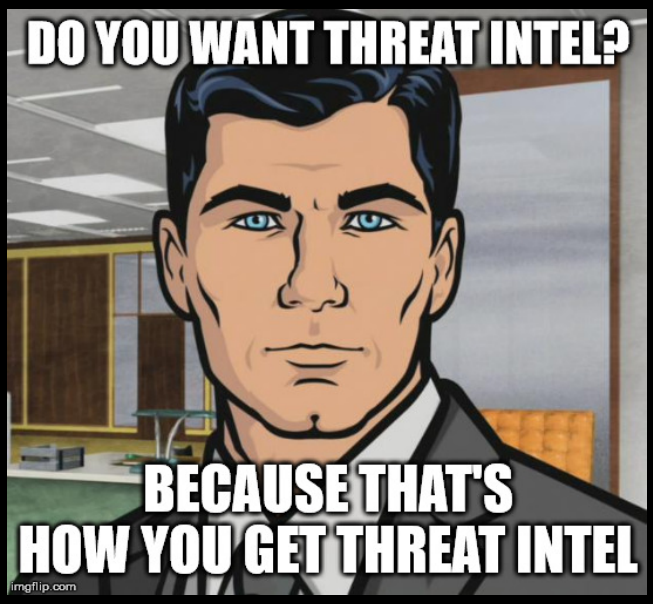
```
User-agent: *
Disallow: /api/
Disallow: /bo/
Disallow: /uploader.jsp
Disallow: /admin/
Disallow: /editor.jsp
```

Sign in

Username or Email Address

Password

Login



Honeypots are dead easy…

Honeypots lie

Lie to the exploit

Web Services

```
<xs:element name="actionCSRImpersonateCustomer">
    <annotation>
        <documentation>
            Allow Phone rep (CSR) to become user. Internal use only.
        </documentation>
    </annotation>
</xs:element>
```

```
<xs:element name="CBCStreamAuthenticator">
    <annotation>
        <documentation>
            Crypto stream generator. Used for creating user tokens.
        </documentation>
    </annotation>
</xs:element>
```

Honeypots buy time

Honeypot data

```
DESCRIBE CC_Info;

+-------------+---------------------+------+-----+---------+----------------+
| Field       | Type                | Null | Key | Default | Extra          |
+-------------+---------------------+------+-----+---------+----------------+
| Cust_ID     | int(10) unsigned    | NO   | PRI | NULL    | auto_increment |
| CC_Num      | varchar(16)         | NO   | UNI | NULL    |                |
| Card_Name   | varchar(75)         | NO   |     | NULL    |                |
| Expires     | date                | NO   |     | NULL    |                |
| CSC         | int(3)              | NO   |     | NULL    |                |
| active_user | tinyint(1) unsigned | NO   | MUL | 1       |                |
+-------------+---------------------+------+-----+---------+----------------+
```

```
DESCRIBE Potential_Explore_Sites;

+-------------+---------------------+------+-----+---------+----------------+
| Field       | Type                | Null | Key | Default | Extra          |
+-------------+---------------------+------+-----+---------+----------------+
| Site_ID     | int(10) unsigned    | NO   | PRI | NULL    | auto_increment |
| LAT         | int(6)              | NO   | UNI | NULL    |                |
| LONG        | int(6)              | NO   |     | NULL    |                |
| Purch_Max   | int(9)              | NO   |     | NULL    |                |
| Purch_Date  | date                | YES  |     | NULL    |                |
+-------------+---------------------+------+-----+---------+----------------+
```

Honeypots are dead easy…

You’re already ready!

Shout out to:
Michael Hogue-Rennie

infosecinnovations: Home
https://www.infosecinnovations.com
I'd love to hear from you. . Fill out the form Cached in touch. . No spam. Ever! Contact.
Send. Research: The lifeblood of our industry. There's so much to ...

```
<link rel='stylesheet' id='contentking-stylesheet-css'  href='https://www.loggl
<link rel='stylesheet' id='et-gf-open-sans-css'  href='https://fonts.googleapis
<link rel='stylesheet' id='et_monarch-css-css'  href='https://www.loggly.com/wp
<link rel='stylesheet' id='loggly-style-css'  href='https://www.loggly.com/wp-c
<link rel='stylesheet' id='tablepress-default-css'  href='https://www.loggly.co
<script type='text/javascript' src='https://www.loggly.com/wp-includes/js/jquer
<script type='text/javascript' src='https://www.loggly.com/wp-includes/js/jquer
<link rel='https://api.w.org/' href='https://www.loggly.com/wp-json/' />
<link rel="EditURI" type="application/rsd+xml" title="RSD" href="https://www.lo
<link rel="wlwmanifest" type="application/wlwmanifest+xml" href="https://www.lo
<link rel='shortlink' href='https://www.loggly.com/?p=76599' />
<link rel="alternate" type="application/json+oembed" href="https://www.loggly.c
<link rel="alternate" type="text/xml+oembed" href="https://www.loggly.com/wp-js
<style type="text/css" id="et-social-custom-css">
```

```
<script type="text/javascript"
src="/scripts/libs/jquery-ui.min.js"></script>
```

x.x.x.x - - [20/Oct/2019:10:27:32 -0500] "GET /scripts/libs/jquery-ui.min.js" 404 7218

404’s as honeypots!

1. Pictures
2. CSS
3. JavaScript files
4. XML Schemas

RECAP

- Honeypots are dead easy
- Overlay honeypots are best.
- Advantages of honeypots
  - They slow attackers down
  - Make for easier detection
  - Make for quicker detection

Conventional Wisdom isn't wise

- Have to be a pen tester when I "grow up"
- Have to do all the things before I do "active defense"

Thank you!

- My wife
- SANS
- You!

INFOSEC
INNOVATIONS

Oh $&@+!!
I finished too early!

MORE HONEY AWESOME!

Honeypots hurt

Honeypots hurt*
(consult your lawyers)

Honeypot zipbomb

```
User-agent: *
Disallow: /api/
Disallow: /backups/
Disallow: /uploader.jsp
Disallow: /admin/
Disallow: /editor.jsp
```

Honeypot PDF

MSFVenom

```
<xs:element name="QuoteGeneratorPDF">
    <annotation>
        <documentation>
            Generate Quote PDF. If no quote ID is
given, send all PDFs associated with current user
        </documentation>
    </annotation>
</xs:element>
```